REMARKS

Applicants thank the Examiner for the thorough consideration given the present application. Claims 1-31 are currently being prosecuted. The Examiner is respectfully requested to reconsider his rejections in view of the amendments and remarks as set forth below.

Rejection Under 35 USC 112

Claims 1-27 stand rejected under 35 USC 112, second paragraph, as being indefinite. This rejection is respectfully traversed.

The Examiner first objects to the term "sufficient time" in claim 1. By way of the present amendment, this limitation has now been changed to "a time long enough." Applicants submit that this limitation is more definite.

The Examiner also objected to the term "substantially" in claims 1 and 6. This term is used to modify "immediately" in the last paragraph of claim 1 and in the second line of claim 6. Applicants have utilized this modifier since it is difficult to provide the invalidation "immediately," since there is a certain amount of time for electronic signals to travel and for the computer to act on the message. Thus, the word "substantially" has been added to indicate that the invalidation occurs as soon as the equipment can make the change. Applicants submit that this is not indefinite and that the use of "substantially" has long been accepted as a modifier in situations where it is physically impossible to perform the act it modifies to the extent required by the unmodified term. Thus, it is often used in chemical formulas to indicate purity of the substance, where it is always impossible to have 100% pure materials. Accordingly, Applicants submit that the use of the term "substantially immediately" clearly indicates that the act occurs as soon as possible. While Applicants believe that the term is definite, if the Examiner prefers, it would be possible to remove the word "substantially" and merely leave the term "immediately" if the Examiner prefers, based on the understanding that the term "immediately" would mean as soon as possible. If the Examiner would prefer a different term, such as "as soon as possible" Applicants are also willing to make such a change. Accordingly, Applicants submit that this rejection is overcome.

Applicants note the Examiner's remark about the misspelling of the word "transitory" on page 2 of the previous Amendment.

Rejection Under 35 USC 103

Claims 1-9, 12, 13, 18, 23, 26 and 27 stand rejected under 35 USC 103 as being obvious over Rowney et al. (U.S. Patent 5,987,140) in view of Oishi (U.S. Patent 6,298,153). This rejection is respectfully traversed.

The Examiner has repeated his previous argument that Rowney et al. shows a method for performing a transaction between entity B and entity A and that Rowney discloses the use of a certificate to verify the approval to entity B. The Examiner admits that Rowney et al. does not teach that the unique transitory insignia is valid for a single transaction and valid only for a sufficient time to complete a transaction. The Examiner also admits that Rowney et al. does not teach invalidating substantially after the validation of the transitory unique insignia.

The Examiner relies on Oishi to teach a certificate that is valid only for a single transaction and valid only for a sufficient time to complete the transaction. The Examiner feels it would have been obvious to modify the system of Rowney et al. so that the certificate is only valid for a single transaction and for a sufficient time to complete the transaction.

First, Applicants submit that it would not be obvious to combine the teachings of Rowney et al. with Oishi. The Oishi teachings deal with an anonymous public key certificate which can be used one time. However, this type of arrangement is different than the electronic commerce arrangement of Rowney et al. Applicants submit that it would not obvious to use the teachings of Oishi in the device of Rowney et al.

Furthermore, Applicants submit that Oishi at best, only teaches the concept that the certificate is used one time and discarded. Thus, even if the teachings of Oishi were added to Rowney et al., the present invention would not be seen.

It should be remembered that in the present invention, when the customer (A) wishes to buy from the store (B), (A) goes to (C) to obtain a digital unique transitory insignia from (C) which can be used for the single transition only and is only valid for the time long enough to complete the transaction. Since the insignia is provided to the customer from the bank (C) the customer provides it to the store so that the store can then verify through the bank that the customer is a valid purchaser. The bank then invalidates the insignia so that it cannot be used again. Thus, the amount of time that the insignia is valid is relatively short, perhaps on the order of seconds.

The bank can invalidate the insignia on the basis of time alone or can cause the invalidation as soon as the purchase is complete or even at the time when the store validates the insignia through the bank. This arrangement differs from the references cited and also from the standard systems used in commerce now. Prior art devices provide an identifier of much longer term to the customer, such as a credit card number or other long term identification number. Using the present invention, the chances for fraud are much reduced due to the short amount of time that the insignia is valid.

Claim 1 now has been amended to make it clear that the verification insignia is a digital insignia. The claim has also been amended to even more clearly point out that the providing of the insignia is for a single transaction and is provided shortly before the transaction. This helps to emphasize the difference over the prior art where the insignia may be valid for a much longer time. This concept has already been stated in that the insignia is defined as "transitory" and also stated to be "for a single transaction and valid only for a time long enough to complete the transaction." However, by adding this phrasing, it now becomes even more clear that the insignia is only obtained immediately before the transaction occurs. The claim already indicates that the insignia is invalidated after the transaction. Applicants submit that this arrangement is not shown in Rowney et al. or the combination of Rowney et al. and Oishi.

It is noted that the Examiner has mentioned on page 4 of the Office Action that the previous arguments against the references relate to features which are not recited in claim 1. In regard to the phrase "associate the payment transaction with a unique transitory insignia", Applicants believe the Examiner is incorrect in this statement. Thus line 5 of claim 1 states "associating the transaction with a digital verification insignia" and line 7 specifies the verification insignia as "a unique transitory insignia". Thus, claim 1 does include this feature. Likewise, new claim 28 also recites this feature in line 7, 8 and 9. Accordingly, Applicants submit that the Examiner is incorrect in her argument that the limitation is not present in the claims.

Thus, claim 1 states that the insignia is a digital unique transitory insignia, that it is valid for a single transaction, that it is valid only long enough to complete a transaction, that it is provided by entity C shortly before the transaction and for the single transaction. The insignia is provided by C to A after A provides to C a secret identification code, and whereupon A provides the insignia to B to verify the approval by C and B then validates the approval, whereupon C invalidates the insignia. This arrangement is not seen in any manner in the prior art cited by the Examiner. Accordingly, Applicants submit that claim 1 is allowable.

The Examiner has relied on the Rowney et al. reference to teach the use of a digital certificate. However, it is noted that in the background section of the Rowney et al. reference, the use of a digital certificate in a secure electronic transaction (SET) is described. However, as is indicated at the end of column 1, Rowney et al. seeks to overcome the problem of customer acceptance to implementing SET and has instead invented a hybrid approach which does not use a digital certificate. Instead, as described near the end of column 2, the merchant can communicate with a customer using a secure socket layer (SSL) which is a protocol used for secure transactions on the Internet and is widely known. Thus, the Examiner's argument that the unique transitory insignia of the present application is similar to Rowney et al.'s digital certificate is incorrect since Rowney et al. do not use a digital certificate. The Applicant submits that Rowney et al. does not describe any item that corresponds to the present digital unique transitory insignia.

Claims 2-27 depend from claim 21 and as such are also considered to be allowable. In addition, each of these claims recite other features which make them additionally allowable. In particular, claims 3-5 discuss the use of a time stamp to identify the insignia, claims 6, 7, 26 and 27 discuss a specific time whereby the insignia is invalidated, claim 8 which discusses particular events recorded by C. Other claims likewise recite other features which make them additionally allowable as well.

Applicants have added new claims 28 and 29 which recite the present invention in different terms. Thus, claim 28 discusses provided a computer based system over an electronic communication network, associating the transaction with a verification insignia where the insignia includes a unique digital code and optionally one or more of a unique identification code and a time stamp, the insignia being provided by C and starting a timer while the insignia is provided to A and invalidating the insignia after it has been validated. In particular, this claim differs from claim 1 in that it relates the various components of the insignia including a time stamp. It also discusses the presence of the timer. Applicants submit that this claim is likewise allowable for the reasons recited above in regard to claim 1 and because the references do not discuss the other features which are not included in claim 1.

Claim 29 depends from claim 28 and as such is also considered to be allowable. In addition, this claim further recites the invalidation of the insignia either when the insignia is presented for validation or after a prespecified time limit. Applicants submit these claims are additionally allowable.

Applicants have also added new claims 30 and 31 which duplicate independent claims 1 and 28 but which add a phrase indicating that the communication channel used for transmitting the unique transitory insignia is a different channel than that used to provide the secret identification code. Thus is possible for the secret identification code to be transmitted over the internet while the unique transitory insignia is forwarded by way of a PDA, a mobile phone, etc. (See page 13, lines 21-29 of the original specification). Thus, another physical device receives the insignia, increasing security. This arrangement is not seen in any of the references so that new claims 30 and 31 clearly define over all of the rejections.

Claims 10, 24 and 25 stand rejected under 35 USC 103 as being obvious over Rowney et al. in view of Oishi and further in view of Puhl (U.S. Patent 6,223,291). Claim 11 stands rejected under 35 USC 103 as being obvious over Rowney et al. in view of Oishi and further in view of Aziz (U.S. Patent 5,732,137). Claim 22 stands rejected under 35 USC 103 as being obvious over Rowney et al. in view of Oishi and further in view of Haber et al. (U.S. Patent 5,136,646). Claims 14, 20 and 21 stand rejected under 35 USC 103 as being obvious over Rowney et al. in view of Oishi and further in view of Franklin et al. (U.S. Patent 5,883,810). Claims 15-17 and 19 stand rejected under 35 USC 103 as being obvious over Rowney et al. in view of Oishi and further in view of Collin (U.S. Patent 4,992,646). The Examiner relies on the third reference in each case to show a specific additional features discussed in the dependent claims. However, Applicants submit that even if these references do show such features, that these claims remain allowable based on their dependency from allowable claim 1. Furthermore, Applicants submit that it would be even less obvious to combine the three references in each case. Applicants submit that the mere showing of a similar feature in the tertiary reference does not teach that it would be obvious to combine this feature along with the features of Oishi into the Rowney et al. device. Accordingly, Applicants submit that these claims are additionally allowable.

Furthermore, Applicants submit that the present invention differs from the cited references in that the present invention deals with a computer based secure electronic communication system which facilitates the exchange of electronic transactions in such way that it is possible to verify online that the customer has the approval and legal rights to perform such transactions. The transaction may specify the right to a physical admittance to a room (such as a special lounge at an airport), a discount at a gas station, admittance to a computer system, payment of a certain amount of money, or verification/authentication of a person or a system, etc. Since security is provided through a unique transitory insignia which is valid for a single transaction and valid only for a time long enough to complete the transaction, it is nearly impossible for an attack to be rendered against the system. As such, the present system can be used not only for secure payments on the internet, but for a number of other applications such as admittance to physical places, discounts, admittance to computers, secure payments, secure parcel delivery, 2-factor authentication, etc. The present invention covers a secure transaction communication system which does not require any software program to be downloaded to a user's computer and does not require issuing a digital certificate to the user. Traditionally, a digital certificate is issued by a certificate authority, for instance a bank. The certificate is downloaded to the customers computer and resides permanently there on a hard disk. A digital certificate is a datafile containing information about the person to whom the certificate is issued, which requires that the persons personal data is checked by the authority before the certificate is issued. Such a check takes normally days to complete. A digital certificate is often valid for 1 year or more, and having a digital certificate stored permanently on the customers hard disk constitutes a possible risk for fraud as the computer can be stolen or used by unauthorized persons. The present invention overcomes these problems.

The solution provided by Rowney et al. cannot prevent the misuse of a credit card number because in Rowney's solution the credit card (which could be a stolen credit card number) is simply transmitted to the merchant computer, which in turn transmits it to the payment gateway for authorization. The payment gateway computer transmit the credit card number to the bank, which will accept and authorize the payment transaction even if it is a stolen credit card number not belonging to the customer. The present invention solves this problem.

The Oishi invention deals with digital certificates and digital signatures and does not discuss secure payments on the Internet. Instead, Oishi is concerned with privacy issues so that users are unconditionally anonymous to verifiers, which is the opposite intent of the present invention. Accordingly, Oishi's invention is from a somewhat nonanalogous art since it does not deal with secure payments on the Internet.

Applicants also wish to point out certain areas of the specification that help to describe various features of the present invention. Thus, page 4, lines 21-32, describe the purpose of the insignia. Likewise, page 5, lines 24-31 discuss the time between the validation of the insignia and the time of invalidation of the insignia as being short as possible. Similarly, page 6, lines 6-10 discuss the instantaneousness of the validation and invalidation.

In regard to this, a time stamp down to the millisecond can be recorded by C at the time that the insignia is sent to A and can even be part of the insignia. This would make it possible to mark the insignia invalid but active at the same time. When the insignia is sent by B to C for validation, C can then time stamp the time of reception of the insignia and, by examining the amount of time which has occurred since the issuance of the insignia, C can determine if the insignia is still valid by not exceeding a predefined number of seconds. The exact number of seconds can be defined by the system and is calculated for each particular application in order to make an attack on the insignia very difficult. If the lifetime of the insignia is small when compared to the time and complexity to carry out an attack, then the insignia in most cases does not need to be protected because the lifetime and validity of the insignia is so short, it would not be possible to carry out such an attack. Furthermore, the insignia can be encrypted which would make an attack nearly impossible. The insignia can include a time stamp and an ID number which identifies the agreement between A and C and also defines the rights, privileges and obligations given thereby.

As is noted at page 6, lines 21-33, time stamps can be recorded by A and C and provided with the insignia so the time stamp cannot be changed by others. An advantage of this is that the legal entity who is going to validate the insignia can determine by evaluating the data included in the insignia how long the insignia has existed and when it was transmitted. This helps to determine potential fraud. Thus, the unique transitory insignia when provided to A always is timed by the computer timer in C and included in the transitory insignia. Therefore, it is possible to determine when the insignia is still valid. This is clearly not disclosed in the references.

Page 7, lines 1-2 and 9-13 point out the use of the time interval as helping to minimize the possibility of fraud. Page 10, lines 15-21 further discuss the possibility of encryption. Page 13, lines 24-29 point out that the use of a secret format can help to avoid others from detecting the insignia. Thus, it should be remembered that a unique transitory insignia is used once and then may be returned to a pool having a large number of insignias from which the insignias can be selected randomly so that it is unpredictable as to which insignia will be used next for a particular customer. Applicants submit that these features are clearly not seen in the references and that the present invention is patentable over the prior art.

Conclusion

In view of the above remarks, it is believed that the claims clearly distinguish over the patents relied on by the Examiner, either alone or in combination. In view of this, reconsideration of the rejections and allowance of all of the claims are respectfully requested.

Dated: January 27, 2006

Respectfully submitted,

By
Joe McKinney Muncy
fo Registration No.: 32,334 #43,368
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant